УДК 004.04

МУХИН В.Е.,
ВОЛОКИТА А.Н.

АНАЛИЗ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПРОВЕДЕНИЯ КОРРЕКТИРУЮЩИХ ДЕЙСТВИЙ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ

Статья посвящена анализу событий информационной безопасности в соответствии с международным стандартом ISO/IEC 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Проведение данного анализа позволит выявить взаимосвязь между событиями информационной безопасности, применить соответствующие меры управления и провести корректирующие действия с целью предупреждения повторного возникновения инцидентов безопасности.

The article is devoted to the analysis of the information security events in accordance with international standard ISO/IEC 27001:2005 “Information technology. Security techniques. Information security management systems. Requirements”. This analysis allows to reveal the relationship between the information security events, to apply the appropriate management mechanisms and to perform the corrective actions for the security incidents recurrence prevention.

Введение

Информационная безопасность компьютерных систем и сетей (КСС) подразумевает сохранение информацией свойств конфиденциальности, целостности и доступности [1]. Построение системы управления информационной безопасностью в соответствии с международным стандартом ISO/IEC 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» позволяет организациям получить следующие преимущества [2]:

- уменьшение и оптимизация стоимости поддержки системы безопасности;
- идентификация информационных активов, определение их владельцев и поддержка в актуальном состоянии перечня активов;
- регулярное выявление угроз и уязвимостей безопасности для существующих бизнес-процессов;
- выявление, оценка и контроль рисков;
- эффективное управление информационными активами предприятия в критичных ситуациях в соответствии с утвержденным планом по восстановлению бизнеса.

Проведение мониторинга и анализа системы менеджмента информационной безопасности является требованием стандарта ISO/IEC 27001.

Мониторинг безопасности представляет собой комплекс мер и мероприятий (технических, организационных и правовых), направленных на реализацию наблюдения, анализа и прогнозирования состояний безопасности сложных систем. Однако, существующие алгоритмы для системам менеджмента информационной безопасности (СМИБ) не позволяют провести комплексную оценку действий злоумышленников, выстроить цепочку реализованных уязвимостей, определить их конечную цель и оценить риски безопасности информационных ресурсов, что может приводить к финансовым потерям, а также повторным успешным атакам на компьютерные системы и сети.

Стандарт ISO/IEC 27001 содержит требования к разработке, внедрению, функционированию, мониторингу и анализу СМИБ, но не содержит готовых алгоритмов, которые могут быть использованы для управления информационной безопасностью.

Таким образом, актуальным является создание новых алгоритмов, обеспечивающих анализ событий информационной безопасности и проведение соответствующих корректирующих действий для своевременного предупреждение инцидентов безопасности.

Алгоритм анализа событий информационной безопасности

На основании анализа существующих подходов и методов мониторинга безопасности предложен новый алгоритм анализа событий

информационной безопасности, в котором формируется взаимосвязь между событиями и выполняется их группировка [3].

Для выявления взаимосвязи между событиями будем использовать коэффициент корреляции, характеризующий зависимость случайных величин. На основании статистических данных мониторинга строится матрица распределения событий информацион-ной безопасности (x_i, x_j), пример которой приведен ниже в виде таблицы 1.

Табл.1. Матрица распределения значений двух факторов.

x_b / x_a	x_{b1}	x_{b2}	..	x_{bm}
x_{a1}	$p_{xa1, xb1}$	$p_{xa1, xb2}$	..	$p_{xa1, xbm}$
..	..	..	$p_{xai, xbj}$	..
x_{an}	$p_{xin, xj1}$	$p_{xin, xj2}$	..	$p_{xin, xjm}$

Где x_a, x_b - события, произошедшие в КСС, между которыми устанавливается возможная зависимость; $x_{a1}..x_{an}$ диапазон возможных значений события x_a; $x_{b1}..x_{bm}$ - диапазон возможных значений события x_b; $p_{xa1,xb1}$ - вероятность нахождения фактора x_a в диапазоне x_{a1}, а фактора x_b в диапазоне x_{b1} [4].

Причем, $\sum_{i,j} p_{xai,xbj} = 1$.

Ряд распределения значений события x_a имеет вид:

x_{a1}	..	x_{an}
$\sum_j p_{xa1,xbj}$	..	$\sum_j p_{xan,xbj}$

Находим математическое ожидание события x_a:

$$MX_a = x_{a1} \cdot \sum_j p_{xa1,xbj} + .. + x_{an} \cdot \sum_j p_{xan,xbj} . \quad (1)$$

Затем находим дисперсию DX через второй начальный момент:

$$\alpha_2(X_a) = x_{a1}^2 \cdot \sum_j p_{xa1,xbj} + .. + x_{an}^2 \cdot \sum_j p_{xan,xbj} , \quad (2)$$

$$DX_a = \alpha_2(X_a) - MX_a^2 , \quad (3)$$

$$\sigma_{x_a} = \sqrt{DX_a} . \quad (4)$$

Аналогично, находится ряд распределения события x_b, суммируя вероятности $p_{xai,xbj}$ по столбцам, а также дисперсия DX_b.

Далее находим математическое ожидание событий x_a и x_b:

$$MX_i X_j = x_{i,1} \cdot x_{j,1} \cdot p_{xi1,xj1} + .. + x_{i,n} \cdot x_{j,m} \cdot p_{xin,xjm} \quad (5)$$

Затем находим значение ковариации x_a и x_b:

$$\begin{aligned} \operatorname{cov}(X_a, X_b) &= M\left[(X_a - MX_a)(X_b - MX_b)\right] = \\ &= MX_a X_b - MX_a \cdot MX_b \end{aligned} \quad (6)$$

На основании полученного значения находится значение коэффициента корреляции событий x_a и x_b:

$$cor_{xa,xb} = \frac{\operatorname{cov}(x_a, x_b)}{\sigma_{xa}\sigma_{xb}} . \quad (7)$$

Коэффициент корреляции характеризует степень зависимости факторов x_a и x_b. При этом положительная корреляция между событиями означает, что при наступлении (увеличении значения) одного события значение другого также имеет тенденцию к возрастанию. Значение положительных коэффициентов корреляции, характеризующих взаимосвязь событий, может быть использовано администратором безопасности при построении графов потенциальных действий и целей субъектов.

Отрицательная корреляция означает, что при возрастании значений одного из событий значение другого события имеет тенденцию к убыванию. Таким образом, данные сведения могут быть использованы для модификации системы безопасности КСС, при которой перераспределение защитных ресурсов будет происходить от объектов, не нуждающихся в защите к объектам, подвергающимся атакам.

Пример использования анализа событий информационной безопасности

На основании разработанного алгоритма анализа событий информационной безопасности предлагается реализация следующих этапов сбора и подготовки данных для принятия решений по управлению безопасностью [5]:

1) **Идентификация активов** – анализ конфигурации фрагмента корпоративной сети (рис.1), проводимый для выявления основных информационных активов (ресурсов), на которые могут быть нацелены атаки злоумышленников.

Для данного примера фрагмента КСС такими основными ресурсами являются база данных СУБД (*R1*), в которой находятся данные о клиентах компании, а также информация об их платежах и задолженностях.

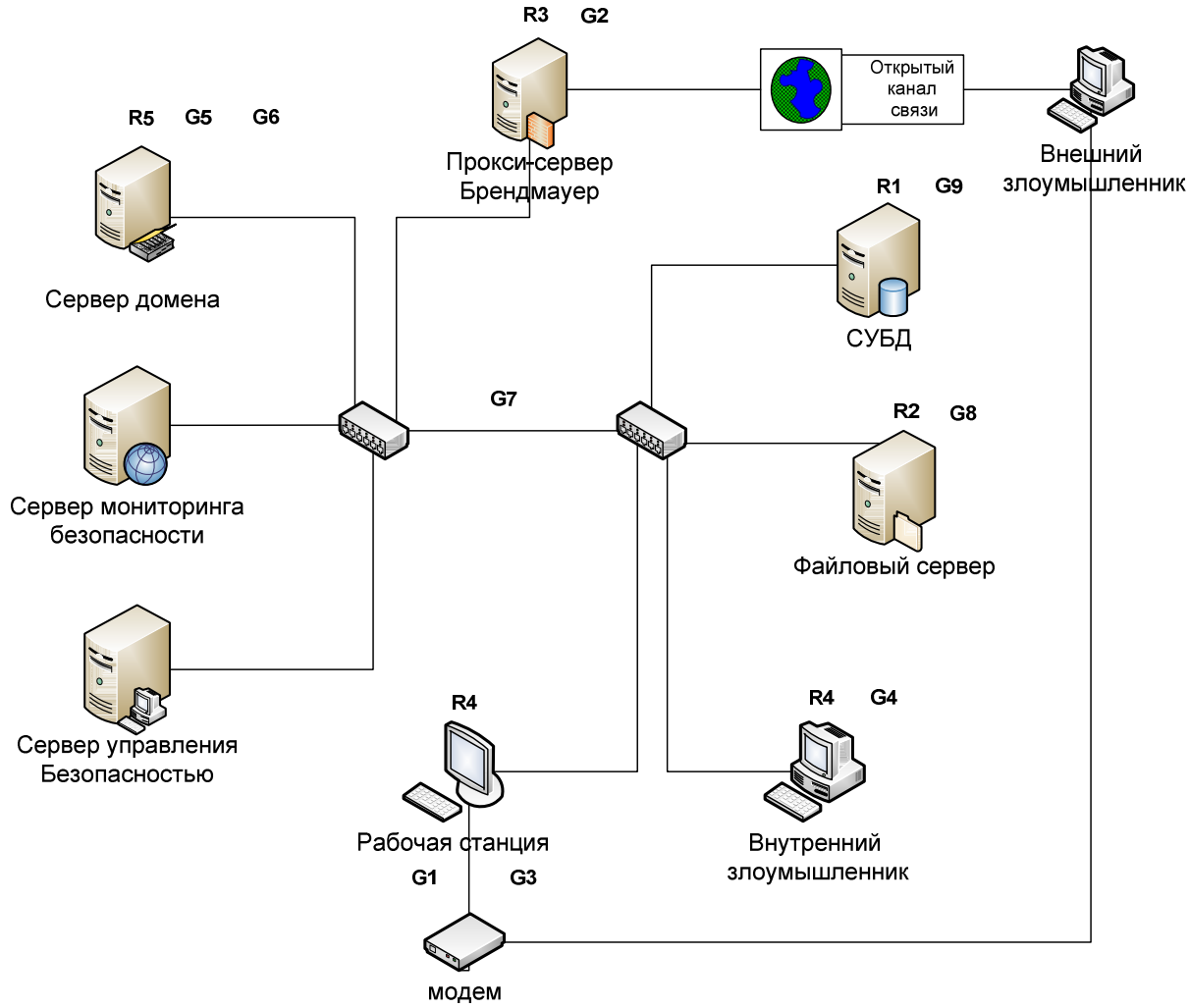

Рис.1. Фрагмент корпоративной сети

Кроме того, критичной является резервная копия данной базы, хранящаяся на файловом сервере (*R2*), а также сервер домена (*R5*). На основании полученной информации формируется вектор информационных ресурсов $r_{1\times f}$. Следует отметить, что выделение основных информационных ресурсов, требующих защиты, проводится на основании данных, полученных от владельцев информации. Собранная информация о конфигурации КСС позволяет приступить к следующему этапу – анализу угроз и уязвимостей данного фрагмента.

2) **Идентификация угроз и уязвимостей** – анализ уязвимостей КСС выполняется на основании топологии сети, статистических данных о событиях в компьютерной системе, полученных с помощью специализированного программного обеспечения, а также сведений об известных вторжениях. На этом этапе строится графовая модель уязвимостей данного фрагмента КСС (рис.2). Вершины графа представляют собой уязвимости, использование которых позволяет оказывать определенное воздействие на компьютерную систему, а дуги показывают возмож-

ность перехода от реализации одной уязвимости к другой.

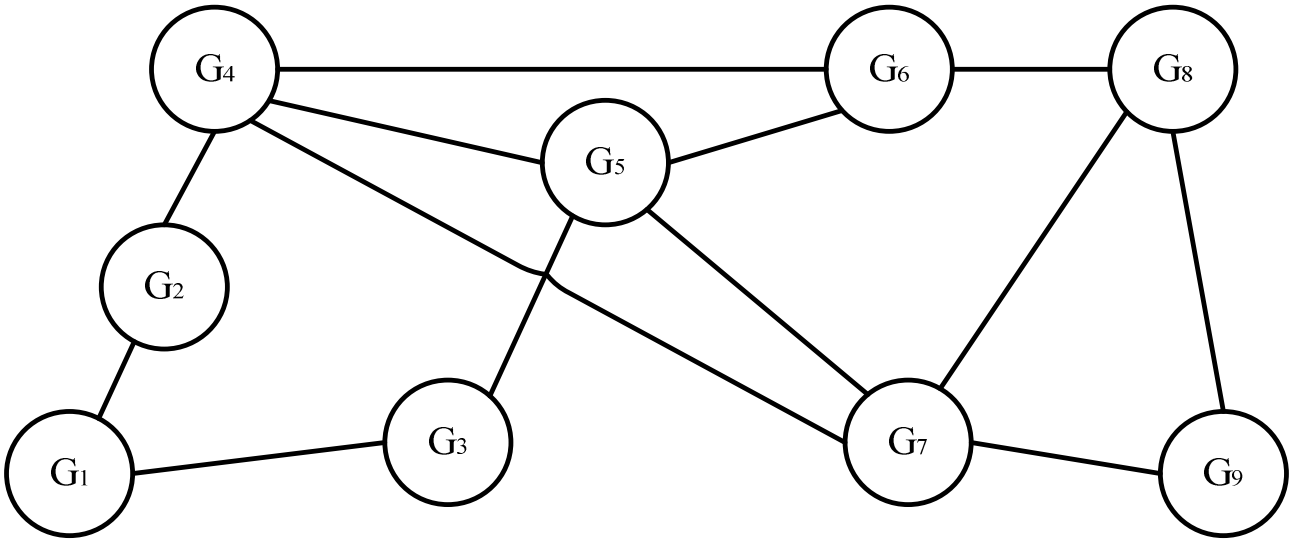

Рис.2. Возможная последовательность реализации уязвимостей

При построения данного графа, кроме приведенных выше формул для расчета взаимосвязи событий безопасности, могут быть использованы экспертные оценки, что вносит некоторый элемент субъективизма.

Например, для данного фрагмента КСС, вершины графа G_i представляют собой следующие уязвимости:

G_1 – открытый канал связи;

G_2 – уязвимости конфигурирования прокси-сервера;

G_3 – незащищенная точка доступа к сети (возможность запуска ПО и доступа к локальным ресурсам – уязвимость в «обе стороны»);

G_4 – уязвимости операционной системы (получение пароля локального администратора с помощью хеш-файла / подбора пароля);

G_5 – уязвимости DNS (получение таблицы DNS, удаленный доступ с помощью поврежденных RPC пакетов);

G_6 – уязвимости сервера домена (чтение активного каталога при инсталляции специализированного программного пакета);

G_7 – уязвимости стека протоколов TCP\IP (передача паролей в незащищенном виде);

G_8 – уязвимости конфигурирования файлового сервера (не отведение защищенной области данных);

G_9 – уязвимости сервера баз данных (возможность не доменной, а sql-аутентификации);

другие.

Определение потенциальных целей злоумышленников позволяет определить соответствующие им действия, с помощью которых данные уязвимости могут быть реализованы.

3) **Анализ этапов и трасс атак** проводится для отслеживания текущей активности злоумышленников и формирования очередности выполняемых ими действий. Для использования приведенных выше уязвимостей злоумышленник может выполнять определенную комбинацию действий a_i приводящую к использованию уязвимостей (Gj) (рис.3) :

a_1 – использование фрагментированных пакетов; (G_1)

a_2 – DOS - атаки; (G_1)

a_3 – несанкционированное подключение к модему; (G_3)

a_4 – локальный анализ log-файлов; (G_4)

a_5 – локальный подбор паролей; (G_4)

a_6 – запуск программ типа «троянский конь»; (G_4)

a_7 – получение IP-адресов и DNS-имен серверов; (G_5)

a_8 – изменение\захват IP-адреса; (G_5)

a_9 – получение полных сведений о доменных пользователях; (G_6)

a_{10} – получение паролей пользователей с помощью анализатора пакетов; (G_7)

a_{11} – копирование / модификация бекапов баз данных; (G_8)

a_{12} – доступ к рабочей базе данных. (G_9).

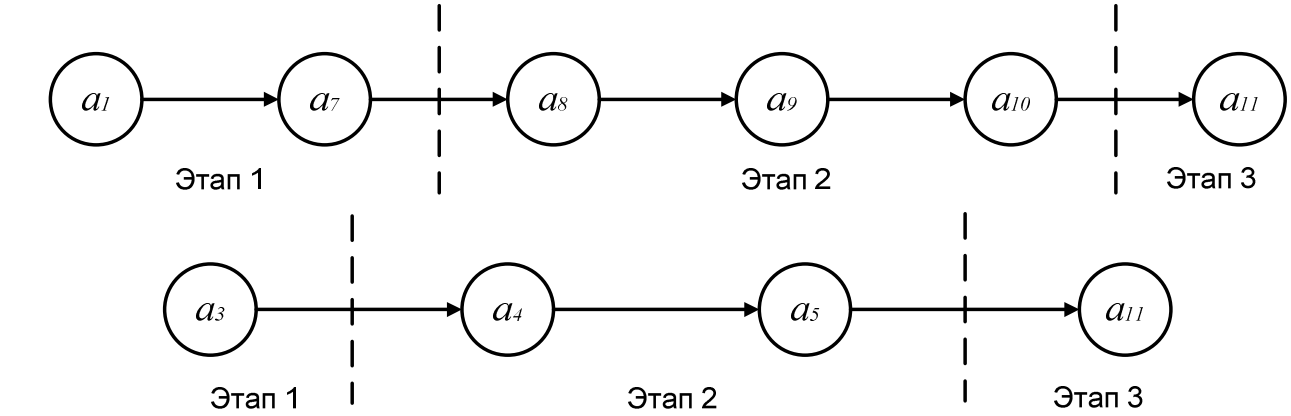

Рис.3. Этапы и трассы атак. Примеры развития 2-х атак

Для контроля событий безопасности и мониторинга действий пользователей необходима подстройка средств обеспечения безопасности, таких как системы обнаружения вторжений, средства защиты (антивирусы, межсетевые экраны, аппаратные средства защиты и контроля доступа) и анализаторы процессов КСС.

4)**Мониторинг событий безопасности** x_i, нуждающихся в дополнительном контроле:

- контроль трафика пакетов протоколов IP и ICMP; (a_1)
- контроль сканирования портов (ответы без запросов); (a_2)
- количество/интервалы подключений; (a_2)
- инициализация подключения к модему; (a_3)
- попытки доступа к log-файлам, журналам регистрации приложений; (a_4)
- контроль неудачных попыток аутентификации; (a_5)
- попытки подключения к службе удаленного реестра; (a_6)
- установка новых служб, помещение программ в автозапуск; (a_6)
- установка специализированных пакетов для доступа к папке “security” объектов домена. (a_9)
- другие.

Таким образом после 4-го этапа определены информационные ресурсы, уязвимости, возможные действия злоумышленников и события безопасности, позволяющие выявлять данные действия. Для этого с помощью средств защиты и проверки состоянии системы, выступающих в качестве агентов-приложений, выполняется сбор информации о происходящих в КСС событиях.

5) **Анализ и оценка рисков** безопасности – проведение анализа рисков реализации угроз безопасности информационных ресурсов позволяет ранжировать ресурсы по степени рисков для КСС.

Уровень рисков безопасности может быть оценен на основе эконометрической модели кредитно-финансовых рисков применительно к задачам защиты информации, обладающей определенной ценностью. Для анализа рисков необходимо сопоставить цели злоумышленника и конкретные ресурсы, подвергаемые атаке (табл.2).

Табл.2. Риски безопасности информационных ресурсов

Ресурсы / Цели	R_1	R_4	R_5
G_6	R_{16}	R_{46}	-
G_8	-	R_{48}	R_{58}

Таким образом, администратор безопасности получает данные о текущей активности по отношению к активам организации.

6) **Выбор мер управления для обработки рисков** безопасности – выполнение соответствующей настройки средств защиты информации. Так, например, целями злоумышленника являются рабочая станция и DNS-сервер. Учитывая ценность информации, а также степень критичности ресурсов администратор безопасности может предпринять следующие варианты действий:

- запретить модемные соединения на рабочих станциях, создать модемный пул;
- повысить защищенность DNS-сервера за счет специализированных средств защиты.

Граф уязвимостей (рис.2) позволяет выстроить цепочку возможных действий злоумышленника, исходя из его текущего положения в пространстве целей (уязвимостей) и текущей активности, а также спрогнозиро-

вать его следующие шаги и определить потенциальные и возможные конечные цели, и, соответственно, возможные действия. Это позволяет контролировать вторжения на их начальной стадии.

На основании построенного прогноза поведения злоумышленников с помощью обратного прохода по графу этапов атак определяются события безопасности, нуждающиеся в дополнительном контроле, а также может быть проведена перенастройка средств защиты.

Для обнаружения несанкционированных действий должны быть обеспечены ведение и хранение в течении определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении анализа событий информационной безопасности. Часы всех систем, покрываемых СМИБ, должны быть синхронизированы с помощью единого источника точного времени. Средства регистрации и данные журналов регистрации должны быть защищены от вмешательства и несанкционированного доступа, действия администратора и системного администратора должны быть регистрируемыми.

Выводы

В соответствии с международным стандартом ISO/IEC 27001 организации должны проводить мероприятия по устранению причин несоответствий требованиям СМИБ с целью предупреждения их повторного возникновения. Применение предложенного анализа событий информационной безопасности позволяет выполнять корректирующие действия в рамках постоянного улучшения системы менеджмента информационной безопасности. Кроме того, полученные результаты могут быть использованы администраторами безопасности для определения потенциальных несоответствий требованиям СМИБ и проведения предупреждающих действий.

Список использованной литературы

1. ISO/IEC 27001:2005 “Information technology – Security techniques – Information security management systems – Requirements”.
2. Дмитриев А. А. ISO/IEC 27001 – Путь к информационной безопасности. Особенности внедрения на отечественных предприятиях.// Das Management, N1, 2009. – с. 36 – 39.
3. Мухин В.Е., Волокита А.Н. Алгоритм оценки вероятности вторжений для средств мониторинга безопасности компьютерных систем. // Системные исследования и информационные технологии, N2, 2007. – с. 47 – 58.
4. Кудрявцев В. Л., Демидович Б. П. Краткий курс высшей математики: Учебное пособие дли вузов. 7-е изд., испр. – М: Наука. Гл. ред. физ.-мат. лит., 1989. – 656 с.
5. Волокита А.Н. Система поддержки принятия решений для средств мониторинга безопасности компьютерных сетей. //Новые технологии, N1(216), 2007. – с. 253 – 258.

Поступила в редакцию 01.12.2009